Amendments to the Drawings

The attached replacement sheet includes changes to Figure 1 and replaces the original sheet that included Figure 1.

Attachment: Replacement Sheet

REMARKS

Reconsideration of this application is respectfully requested in view of the foregoing amendment and the following remarks.

Claims 1-30 were pending in this application. In the Amendment, Applicant has amended claims 1, 12, 19, and 22 and has not canceled or added any claims. Accordingly, claims 1-30 will still be pending upon entry of this Amendment.

In the Office Action mailed November 17, 2006, the Examiner rejected claims 1-30 under 35 U.S.C. § 101 as directed to non-statutory subject matter. The Examiner rejected claims 1-7, 9-17, 19-28, and 30 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 7,127,743 to Khanolkar et al. ("Khanolkar"). The Examiner also rejected claims 8, 18, and 29 under 35 U.S.C. § 103(a) as being unpatentable over Khanolkar in view of page 9, line 6 of paragraph [0030] to page 10, line 2 of the present specification ("Alleged Admitted Prior Art"). The Examiner also objected to claim 19 for informalities and to Figure 1 for not showing the word "network" for element 150. To the extent that the §§ 102 and 103 rejections might still be applied to the presently pending claims, Applicant respectfully traverses the rejections.

The following remarks are organized under subheadings corresponding to the rejections and objections.

35 U.S.C. § 101: Claims 1-30

The Examiner rejected independent claims 1 and 12, and their respective dependent claims 2-11 and 13-21, as reciting a "system" that could be reasonably interpreted as unpatentable software, per se. In response, Applicant has amended independent claims 1 and 12 to recite that the system is a computer-implemented system. Applicant therefore respectfully

submits that claims 1-21 are directed to statutory subject matter and requests withdrawal of this rejection.

With respect to claims 22-30, the Examiner rejected the claimed method as not resulting in a tangible result. Applicant respectfully traverses this rejection and submits that the claimed ultimate step of "sounding an alarm" is indeed a tangible result, which the specification at ¶¶ [0028-29] explains could be an email, a telephone call, a display on a graphical user interface (GUI), a sound, or any available communication type. This communication is unquestionably a tangible result. Nevertheless, to emphasize this feature, Applicant has amended independent claim 22 to recite generating an alarm communication. Applicant therefore respectfully submits that independent claim 22, and dependent claims 23-30 by virtue of their dependency, recite a method culminating in a tangible result, and respectfully requests withdrawal of this rejection.

35 U.S.C. § 102(e): Claims 1-7, 9-17, 19-28, and 30

The Examiner rejected independent claims 1, 12, and 21, in part, based on column 2, lines 25-44 of Khanolkar, which discloses discrete software modules that receive and process log data from various network devices, and noted that Applicant's specification at ¶ [0017] describes both proxy and central loghosts as independent modules that can run on the same system. In view of this broad interpretation of the claimed invention, Applicant has amended claims 1, 12, and 21 to emphasize that the proxy loghost and the central loghost are remote from each other and communicate over a network. Support for these amendments can be found in the application, for example, at ¶¶ [0014-15] of the specification and in Figure 1. Communication between the proxy loghost and the central loghost can be encrypted and facilitated by a secure shell daemon. (*See, e.g.*, ¶ [0016], lines 6-7 and ¶ [0020], lines 1-2 of the specification.)

In contrast, Khanolkar fails to teach or suggest this configuration of the proxy loghost and the central loghost, and instead teaches the opposite, describing the event parsers 54 and event manager 55 as part of the same system 10 and same event handling subsystem 50, as shown in and described with reference to Figure 2. The Examiner acknowledged as much at page 8, lines 9-10 of the Office Action.

In addition, with respect to claim 9, the amendments to its base claim 1 make clear that the log files and the events are stored separately at the proxy loghost and central loghost, respectively. This feature is distinguishable over Khanolkar, which again teaches event parsers 54 and event manager 55 as part of the same event handling subsystem 50 and teaches database 58 as storing only event objects (not log data). (Column 7, lines 10-12 and lines 23-36.)

Applicant has further amended independent claim 12 to recite that the central loghost receives and analyzes log files *and* events. As suggested by the Examiner's interpretation of the previous form of this limitation, Kahnolkar fails to teach or suggest a central loghost that receives log files and events, and instead only teaches event manager 55 as receiving event objects.

For the above reasons, Applicant respectfully submits that amended independent claims 1, 12, and 22 are patentable over Kahnolkar and that dependent claims 2-11, 13-21, and 23-30 are also patentable due at least to their dependence on an allowable base claim.

35 U.S.C. § 103(a): Claims 8, 18, and 29

In rejecting claims 8, 18, and 29, the Examiner relied on Khanolkar and Alleged Admitted Prior Art from the Applicant's disclosure at page 9, line 6 of paragraph [0030] to page

10, line 2. Applicant respectfully traverses the Examiner's interpretation of the Alleged Admitted Prior Art.

At pages 13-14 of the Office Action, the Examiner correctly noted that Khanolkar is "silent on wherein the log files are received from a host-based intrusion detection system," but then relied on an overstated interpretation of the Alleged Admitted Prior Art to cure Khanolkar's deficiency. Contrary to the Examiner's interpretation, the cited sentence does not admit that log files *are received* from a host-based intrusion detection system. It merely admits that host-based intrusion detection systems exist ("to the extent...host-based systems have already been implemented"), which is consistent with the discussion of such existing systems in the "Background of the Invention" section at paragraph [0004]. However, the remainder of the cited sentence, which describes the present invention and is indeed part of the "Detailed Description" of the invention section of the specification, explains that log files can be forwarded to a proxy loghost, *i.e.*, the files are *received from* a host-based intrusion detection system. Therefore, Applicant's disclosure merely admits that host-based intrusion detection systems exist, but describes the *transmission* of log files between the existing host-based intrusion detection systems and the proxy loghost as part of the claimed invention.

Applicant therefore respectfully submits that the Alleged Admitted Prior Art fails to cure the deficiencies of Khanolkar and that the rejection of claims 8, 18, and 29 should be withdrawn.

Objection to Claim 19

As required by the Examiner, Applicant has amended claim 19 to depend from claim 12 and therefore respectfully requests withdrawal of this objection.

Objection to Figure 1

As required by the Examiner, Applicant is submitting herewith a replacement drawing sheet amending Figure 1 to show the word "network" for element 150. Applicant therefore respectfully requests withdrawal of this drawing objection.

In view of the foregoing all of the claims in this case are believed to be in condition for allowance. Should the Examiner have any questions or determine that any further action is desirable to place this application in even better condition for issue, the Examiner is encouraged to telephone Applicant's undersigned representative at the number listed below.

PAUL, HASTINGS, JANOFSKY & WALKER LLP
875 15th Street, N.W.
Washington, D.C. 20005
Tel: 202/551-1700

Respectfully submitted,

Date: May 16, 2007

By: _____
Michael Bednarek
Registration No. 32,329

Attachment: Replacement Drawing Sheet

MB/SPA/ggb
Customer No. 36183